CLAIMS

What is claimed is:

1. A method of ensuring a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of:

obtaining a seed pool comprising a plurality of bits for generating the random number;

remotely storing a seed pool backup of the seed pool via a network; and

restoring the seed pool backup to local memory following a power loss event causing loss to the seed pool.

2. The method of claim 1, wherein the act of remotely storing the seed pool comprises the act of periodically storing the seed pool backup on a remote storage device.

3. The method of claim 2, wherein the act of periodically storing the seed pool backup comprises the act of executing a backup event at a backup interval based on a write cycle characteristic of the remote storage device.

4. The method of claim 1, comprising the act of modifying the seed pool backup with additional random bits to ensure randomness for generating the random number.

5. The method of claim 4, wherein the act of modifying the seed pool backup with additional random bits comprises the act of capturing one or more bits of data from a free-running timer.

6. The method of claim 4, wherein the act of modifying the seed pool backup with additional random bits comprises the act of capturing one or more bits of data from a local hardware device.

7. The method claim 1, wherein the act of restoring the seed pool backup comprises the act of automatically retrieving the seed pool backup via the network upon restoring power to the cryptographic security subsystem.

8. The method of claim 7, wherein the act of automatically retrieving the seed pool backup comprises requesting the seed pool backup from a remote management system.

9. The method of claim 1, wherein the power loss event is a battery failure resulting in memory loss of the seed pool from the local memory.

10. The method of claim 1, wherein the act of restoring the seed pool backup comprises the act of transmitting the seed pool backup from remote storage to the local memory via the network following a battery replacement for the local memory.

11. A method of restoring a seed pool for generating a random number for a security system, the method comprising the acts of:

transmitting a periodically stored backup of the seed pool to the security system via a network following loss of the seed pool from the security system; and

repopulating local memory of the security system with the periodically stored backup for use in generating the random number.

12. The method of claim 11, comprising the act of modifying the periodically stored backup with additional random bits to ensure randomness.

13. The method of claim 12, wherein the act of modifying the periodically stored backup with additional random bits comprises the act of capturing one or more bits of data from one or more local hardware components.

14. The method of claim 11, comprising the act of periodically storing the seed pool in a remote storage device via the network at an interval based on a write cycle characteristic of the remote storage device to maintain availability of the seed pool as the periodically stored backup.

15. The method claim 11, wherein the act of transmitting the periodically stored backup comprises the act of transferring the periodically stored backup to the security system after restoring battery power to the security system.

16. The method of claim 15, wherein the act of transferring the periodically stored backup comprises automatically initiating a seed pool restoration event using the periodically stored backup stored on a remote server after restoring battery power by replacing a battery for the local memory of the security system.

17. A security system, comprising:

a security subsystem, comprising:

a power dependent memory device;

a limited life battery for the power dependent memory device;

a seed pool stored on the power dependent memory device, wherein the seed pool comprises a plurality of random bits; and

security logic configured to generate a cryptographic key to establish a secure communication session between the electronic device and an external device, wherein the security logic generates the cryptographic key from the seed pool; and

a security backup system, comprising:

a remote storage device;

a backup control module configured for periodically storing a backup of the seed pool in the remote storage device; and

a restoration control module configured for repopulating the power dependent memory device with the backup following replacement of the limited life battery.

18. The system of claim 17, comprising a remote security interface configured for interacting with the security subsystem and the security backup system. .

19. The system of claim 17, wherein the security backup system comprises a seed

pool modification module configured for capturing one or more bits of data from a hardware component and adding the one or more bits to the backup.

20. The system of claim 17, wherein the security backup system comprises an automation module configured for automatically initiating repopulation of the memory device with the backup.